Mise en place d'un AAA

Objectifs de cette séquence d'exercices :

- Expliquer le fonctionnement d'un AAA
- Implémenter un server AAA pour l'authentification de périphériques et services
- Être capable d'analyser un fichier de log d'un serveur RADIUS et d'en déduire des informations de dépannage comme règle d'autorisation, protocole d'authentification, etc.

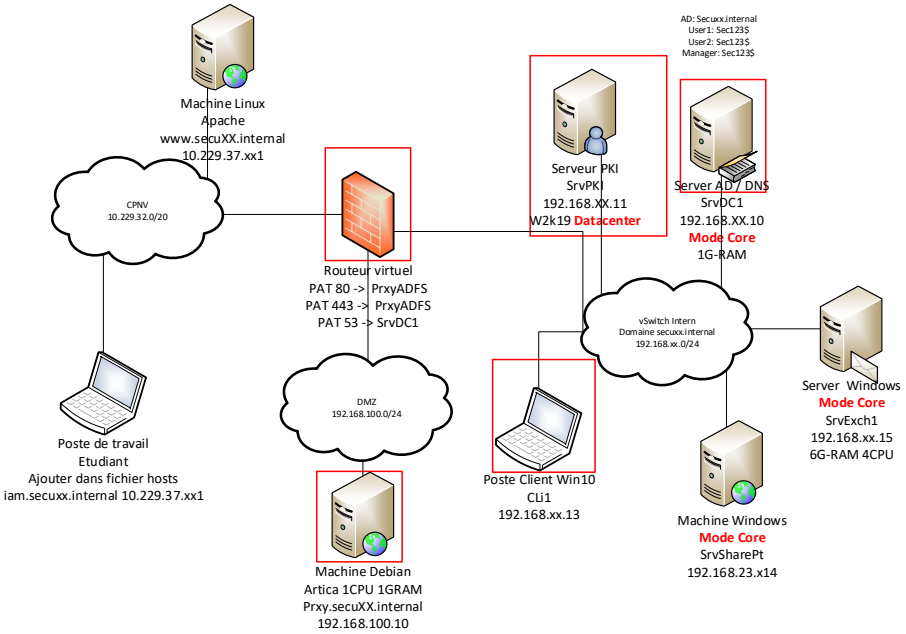
Console à utiliser :

- Outil de management Mikrotik : `winbox.exe`
- Outils de configuration Network Policy Server: `nps.msc` (il faut au-préalable ajouter le service)
- Outils de diagnostic radius : `ntradping.exe`

Documents/fichiers :

- https://blog.devensys.com/aaa-authentication-authorization-accounting/
- https://mivilisnet.wordpress.com/2018/10/01/how-to-integrate-your-mikrotik-router-with-windows-ad/
- https://www.commentcamarche.net/contents/91-radius
- https://techexpert.tips/fr/mikrotik-fr/mikrotik-authentification-active-de-lannuaire/
- https://ntradping.apponic.com/
- https://windowsserver.uservoice.com/forums/295059-networking/suggestions/35724043-fix-default-nps-firewall-rules-for-server-2019
- http://www-igm.univ-mlv.fr/~dr/XPOSE2003/Mandille/Radius.htm#_Toc66100285
- https://blog.pingex.net/comprendre-radius-part1-protocole/
- https://social.technet.microsoft.com/Forums/windows/en-US/45aa3000-c32b-483b-8d6e-565b56b163fc/how-to-check-the-nps-logs-in-the-event-viewer
- https://wiki.squid-cache.org/ConfigExamples/Authenticate/Radius

Schéma :
Machines nécessaires pour le module sont entourées en rouge



1 – Analyse infrastructure:

Concept d'une authentification centralisée de type AAA

- Définir le concept d'un AAA
- Définir le fonctionnement d'un AAA
- Définir les ports utilisés pour l'authentification Radius
- Définir trois cas d'application d'un AAA

2 – Mise en place du server AAA:

Pour un support complet du protocole Radius, il est nécessaire de mettre à jour votre Mikrotik vers la dernière version stable. Pour des raisons de séparation des services, il est préférable d'installer le serveur NPS (Radius de Windows) sur le serveur PKI (voir schéma).

Cahier des charges :

7. En tant que responsable de la sécurité, je veux qu'uniquement les flux identifiés (dans l'exercice précédent sur la DMZ, ainsi que les nouveaux flux identifiés dans cet exercice) soit autorisé à traverser le routeur, dans le but de protéger l'infrastructure d'accès non autorisés.

8. En tant que responsable de la sécurité, je veux que mon routeur (Mikrotik) puisse être consulté en lecture seul par les utilisateurs du groupe secu_net_admin par l'utilisation d'un protocole AAA, dans le but d'accroitre la sécurité et la granularité des accès.

9. En tant que responsable de la sécurité, je veux que l'ensemble des utilisateurs du domaine puissent surfer au travers du proxy de manière authentifiée par Radius, dans le but de répondre au besoin de traçabilité des accès vers internet et d'obtenir des logs légaux à présenter en cas d'enquête.

3 – Analyse de logs :

Trouver les emplacements des différents fichiers de log et événements du RADIUS. Analyser le contenu des traces de l'application RADIUS et en déduire quel est le protocole d'authentification utilisé et quel pourrais être vos recommandations.